IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

registering, at an authentication server, unique identification information corresponding to a mobile information terminal, the unique information including a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal;

presenting, from the authentication server to said mobile information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively;

transmitting, from said mobile information terminal to said authentication server, a request to connect to the authentication server;

transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature;

verifying an identity of the authentication server at the mobile information terminal based on the received certificate;

generating, at a Web browser of the mobile information terminal, a secret key based on a result of the verification;

encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server;

transmitting the encrypted secret key from the mobile information terminal to the authentication server;

receiving, at the authentication server from said mobile information terminal, the unique identification information as encrypted by said secret key at the ~~a predetermined encryption algorithm by a~~ Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network;

determining, at the authentication server, whether said unique identification information received from said mobile information terminal is registered with said customer database;

sending a notification from the authentication server to said content providing server by which said requested site is produced, that starting of service provision for said mobile information terminal be permitted, if the unique identification information is found registered with said customer database;

registering, at the authentication server, said requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server; and

notifying, to said mobile information terminal from said authentication server, a completion of said registration.

Claim 2 (Canceled).

Claim 3 (Previously Presented): The user authentication method according to claim 1, wherein,

when registering said site access information user authentication is performed on the basis of said unique identification information and said mobile information terminal is requested to make display for prompting said user to enter a password of the user.

Claim 4 (Previously Presented): The user authentication method according to claim 3, wherein,

in the registering a charging server is instructed to charge said user for the use of a service provided by said content providing server associated with said site access information at the time of registering said site access information.

Claim 5 (Previously Presented): The user authentication method according to claim 4, wherein,

in the registering, confirming, before instructing said charging server for the charging, that said user is a registered user of said charging server is included.

Claim 6 (Canceled).

Claim 7 (Previously Presented): The user authentication method according to claim 1, wherein

the unique identification information is read, by said Web browser, from a flash memory installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser.

Claim 8 (Canceled).

Claim 9 (Currently Amended): A user authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

means for registering unique identification information corresponding to said mobile information terminal, the unique information including a manufacturer code identifying the

manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal;

means for presenting, to said mobile information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively;

means for receiving a request to connect from the mobile information terminal;

means for transmitting a certificate to the mobile information terminal, the certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature;

means for receiving a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web browser at mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate;

means for receiving, from said mobile information terminal, the unique identification information as encrypted by said secret key at the ~~a predetermined encryption algorithm by a~~ Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network;

means for determining whether the unique identification information received from said mobile information terminal is registered with said customer database;

means for sending a notification to said content providing server, by which said requested site is produced, that starting of service provision for said mobile information terminal be permitted, if the unique identification information is found registered with said customer database;

means for registering the requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server; and

means for presenting, to said mobile information terminal, a completion of said registration.

Claim 10 (Canceled).

Claim 11 (Previously Presented): The user authentication server according to claim 9, wherein

the unique identification information is read, by said Web browser, from a flash memory installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser.

Claim 12 (Canceled).

Claim 13 (Currently Amended): A user authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

a registering module configured to register unique identification information corresponding to the mobile information terminal received from the mobile information terminal with a customer database of said authentication server, the unique information including a manufacturer code identifying the manufacturer of the mobile information terminal and an identification code unique to the mobile information terminal;

an interface configured to present, to said mobile information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively;

an interface configured to receive a request to connect to the user authentication server from the mobile information terminal;

an interface configured to transmit a certificate including a public key of the user authentication server, an expiration date of the certificate and a digital signature to said mobile information terminal;

an interface configured to receive a secret key from the mobile information terminal that is encrypted using the public key of the user authentication terminal, the secret key being generated by a Web browser at the mobile information terminal after verifying an identity of the authentication server at the mobile information terminal based on the received certificate;

an interface configured to receive, from said mobile information terminal, the unique identification information as encrypted by said secret key at the ~~a predetermined encryption algorithm by a~~ Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network;

a determination module configured to determine whether the unique identification information received from said mobile information terminal is registered with said customer database;

an interface configured to transmit a notification to said content providing server, by which said requested site is produced, that starting of service provision for said mobile information terminal be permitted, if the unique identification information is found registered with said customer database by the determination module;

a registering module configured to register the requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server; and

an interface configured to present, to said mobile information terminal, a completion of said registration.

Claim 14 (Previously Presented): The authentication server according to Claim 13, wherein the recommended menu including a plurality of official site access information includes a plurality of hierarchical levels of categories.

Claim 15 (Previously Presented): The authentication server according to Claim 13, wherein the customer database is configured to store a name, age, birthday, gender and address corresponding to a user.

Claim 16 (Previously Presented): The authentication server according to Claim 15, wherein the authentication server uses at least one of the name, age, birthday, gender and address corresponding to a user to generate the recommended menu.

Claim 17 (Previously Presented): The authentication server according to Claim 13, wherein the personal menu includes a plurality of icons, each of which correspond to a link to a website external to the authentication server.

Claim 18 (Previously Presented): The authentication server according to Claim 13, wherein the authentication server and the content providing server are remotely connected via the Internet.